Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89

REPLY COMMENTS OF COMSOVEREIGN CORPORATION

COMSovereign Holding Corp. ("COMSovereign")[1] respectfully submits the following reply comments on the Federal Communications Commission's ("FCC" or "Commission") *Further Notice of Proposed Rulemaking* in the above-captioned proceeding.[2] COMSovereign applauds the Commission's efforts to identify and minimize emerging national security risks to the information and communications technology and services ("ICTS") supply chain through a collaborative approach that incorporates insight from private and public stakeholders alike. As a proud U.S.-based company, COMSovereign joins commenters to this proceeding in supporting the Commission's efforts to secure the ICTS supply chain. If the Commission takes additional steps to require removal and replacement of existing communications equipment and services, the Commission should ensure that adequate funding is available for that effort.

[1] COMSovereign is a publicly traded, U.S.-based, small business with a wide portfolio of 5G-related telecommunications and technology companies, including Dragonwave-X, Drone Aviation Corporation, InduraPower, Lextrum, Silver Bullet Technology, and VEO. This diverse array of organizations provides products and services for both telecommunications companies and federal and state agencies alike.

[2] *In re Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs; Huawei Designation; ZTE Designation*, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423 (2019) ("*FNPRM*").

I. COMSOVEREIGN IS A LEADING U.S.-BASED PROVIDER OF NEXT-GENERATION TECHNOLOGIES.

Through its strategic acquisitions and organic research and development efforts, COMSovereign has become a leading pure-play American communications provider capable of actively deploying wireless microwave, 4G, LTE Advanced, and 5G-NR telecommunications applications. COMSovereign's capabilities allow it to supply some of the largest telecommunications and technology companies, and support the second largest installation base of telecom backhaul equipment in the U.S. COMSovereign's subsidiaries also have an established track record of providing products and services to agencies such as the Department of Homeland Security and the Department of Defense.

COMSovereign and its portfolio companies understand that a dependable chain of custody is just as important as the origin of hardware and software components. Specifically, it is crucial that these items are not only sourced correctly, but that they are not counterfeited or compromised by a third party in the ICTS chain. Therefore, COMSovereign and its affiliated companies develop and produce much of their own hardware and software in proprietary North American facilities.

COMSovereign has also developed a core set of trusted partners equally committed to assuring an accurate chain of custody to provide outsourced materials. COMSovereign and its affiliated companies prioritize using well-known partners with a history of quality, and quality assurance that are based in the U.S. and allied countries. All of COMSovereign's partners are established entities, and most of them do business directly with the Department of Defense. COMSovereign takes supply chain security seriously and is encouraged that the FCC is probing these important issues as well.

II. COMSOVEREIGN JOINS COMMENTERS IN SUPPORTING THE COMMISSION'S EFFORTS TO SECURE THE ICTS SUPPLY CHAIN FROM EMERGING NATIONAL SECURITY THREATS.

The record reflects strong support for the Commission's efforts to safeguard the security and integrity of America's communications infrastructure.[3] COMSovereign is encouraged by the FCC's initiatives to secure U.S. telecommunications networks so that next-generation technologies may be safely deployed. American networks support far more than calling, email, and social media capabilities – they represent the information backbone supporting hospitals, first responder communications, power grid infrastructure, and our entire economy.[4] It is of paramount importance that these networks are secure.

Providing foreign adversaries access to American digital infrastructure creates the possibility of denial of service attacks by remotely disabling or rendering inoperable network routers, core switches, and wireless equipment. Another risk is unauthorized access to data. U.S. networks are responsible for over half of the more than 2.5 quintillion bytes of data generated online each day. Much of this data contains sensitive personal information, trade secrets, and classified government information. Unauthorized access through exploitation of

---

[3] *See, e.g.*, Comments of the Telecommunications Industry Association, WC Docket No. 18-89, at 2 (filed Feb. 3, 2020) ("TIA Comments") ("Securing the [ICTS] supply chain will be one of the main challenges to overcome in deploying secure 5G technologies and services. Accordingly, TIA supports the FCC's actions in this docket. . . ."); Comments of CTIA, WC Docket No. 18-89, at 2-3 (filed Feb. 3, 2020); Comments of Competitive Carriers Association, WC Docket No. 18-89, at 1-2 (filed Feb. 3, 2020); Comments of NCTA—The Broadband Association, WC Docket No. 18-89, at 1-3 (filed Feb. 3, 2020); Comments of Triangle Communications System, Inc., WC Docket No. 18-89, at 1 (filed Feb. 3, 2020).

[4] As demonstrated by the Sandworm exploits perpetrated by Russian hackers beginning in 2014, the viability of national utility grids is entirely dependent on network security. Andy Greenberg, *Russia's 'Sandworm' Hackers Also Targeted Android Phones*, Wired (Nov. 21, 2019), https://www.wired.com/story/sandworm-android-malware/.

either hardware or software vulnerabilities can cause billions of dollars in economic losses and render networks susceptible to espionage and cyber warfare. Accordingly, COMSovereign supports the efforts of the FCC and its government partners to secure the American ICTS supply chain from existing and emerging threats.

III. IF THE COMMISSION ADOPTS A REMOVAL AND REPLACEMENT REQUIREMENT, IT SHOULD MAKE ADEQUATE FUNDING AVAILABLE.

If the Commission institutes a "rip-and-replace" program for communications equipment and services, COMSovereign encourages it to make adequate funding available for this endeavor. In developing a reimbursement fund, the FCC should carefully account for the full cost of such a project.[5] The COMSovereign team has participated in prior government replacement initiatives and understands that these programs are both time-consuming and often incur significant deployment costs beyond the replacement of the components themselves. For example, project costs will include technology assessments to ensure the correct fit and functionality of new equipment, evaluation and resolution of integration issues to verify compatible operation of new equipment, and service outages during equipment replacement. COMSovereign respectfully requests that the Commission take into consideration the complete scope of the program's activities, including proposed equipment and software replacement efforts, when making budget calculations.

Moreover, the FCC should ensure that the reimbursement program has sufficient funding to allow carriers of all sizes to purchase the most recent technology from American sources, and/or provide tax and other incentives to do so. In addition to promoting secure networks,

[5] As TIA suggests, the Commission should "consult with equipment manufacturers and 'trusted suppliers' for assistance in determining a proper estimate for the total cost of the proposed reimbursement program." TIA Comments at 10.

enabling purchase of cutting-edge technology from American sources also will benefit the U.S. economy in several ways. First, incentivizing investment in a skilled American workforce will augment the country's capacity to produce critical infrastructure domestically and generate a multitude of skilled high-value jobs. Second, encouraging the purchase of American technologies can support world-class onshore manufacturing capabilities and provide a strategic source for future networks. Third, supporting American-made equipment and services will help the U.S. telecommunications industry in achieving global leadership in the expanding digital economy.

IV. CONCLUSION

COMSovereign is encouraged by the Commission's efforts to safeguard U.S. communications infrastructure. To further the Commission's goals of securing the ICTS supply chain and protecting against threats from foreign adversaries, COMSovereign urges the Commission to ensure that any "rip-and-replace" program be accompanied by sufficient reimbursement mechanisms.

Respectfully submitted,

By:_____

Dustin H. McIntire, PhD
Chief Technology Officer
COMSovereign Holding Corp.

March 3, 2020